

REMARKS

This amendment is responsive to the Office Action of April 27, 2009. Reconsideration and allowance of **claims 1-4 and 8-16** are requested.

The Office Action

Claim 14 was rejected under 35 U.S.C. 112, second paragraph.

Claims 1-4 and 8-11 were rejected under 35 U.S.C. 103(a) as being unpatentable over Jutzi et al. (U.S. Patent Application Publication 2003/0005301) in view of Parr (U.S. Patent No. 5,287,374) in further view of Suzuki (U.S. Patent No. 6,463,445).

Claims 12-13 were rejected under 35 U.S.C. 103(a) as being unpatentable over Jutzi et al. in view of Parr in further view of Suzuki in further view of Matyas Jr. et al. (U.S. Patent No. 7,010,689).

Claim 14 was rejected under 35 U.S.C. 103(a) as being unpatentable over Jutzi et al. in view of Parr in further view of Suzuki in further view of Ko et al. (U.S. Patent Application Publication 2003/0100299).

Claim 15 was rejected under 35 U.S.C. 103(a) as being unpatentable over Jutzi et al. in view of Parr in further view of Suzuki in further view of Henderson et al. (U.S. Patent No. 6,353,666) in further view of Weinstein et al. (U.S. Patent No. 7,233,688).

Background

The present application is directed to a method of determining whether an encoded signal has been encoded by a particular type of encoder. The method comprises the steps of receiving at least a part of the encoded signal; decoding the received signal using a decoder which performs the reverse operation of the particular type of encoder, deriving a fingerprint from the decoded signal; comparing the derived fingerprint with fingerprints stored in a database; and concluding whether the encoded signal has been encoded with the particular type of encoder based on whether the derived fingerprint corresponds to one of the fingerprints stored in the database.

The above description of the present application is presented to the Examiner as background information to assist the Examiner in understanding the application. The above description is not used to limit the claims in any way.

The References of Record

Jutzi et al. is directed to an apparatus and method for enabling secure content decryption within a set-top box. The method includes performance of security authentication of a content driver by a content decryption component in order to verify an identity of the content driver as a secure content driver. The content decryption component receives an encrypted content stream from the secure content driver and performs integrity authentication of a run-time image of the secure content driver. While integrity authentication of the secure content driver is verified, the content decryption component streams decrypted content to the secure content driver to enable playback of the decrypted content to a user.

Parr is directed to a receiver for use in digital cellular communication systems determines the type of data transmitted without having to decode the data. There are a limited number of valid code sequences less than the total possible number of code sequences for a transmission of the same number of bits. This characteristic is used to identify the type of encoding without decoding the received information.

Suzuki is directed to a multimedia information retrieval system and method including automatic format conversion. The system and method comprises a data structure that is associated with each multimedia bitstream. The data structure identifies the encoding format used in the multimedia bitstream which is originated by a contents server. An automatic format conversion process then queries information from the client and also receives the data structure identifying the encoding format. The client information identifies the decoding format. The automatic format conversion determines the transcoding process required for converting the bitstream from its encoded format to the format recognized by the client system.

Maytas et al. is directed to a method, system and computer program product for controlling access to digital data in a file by obtaining a passphrase from a user and generating a personal key based on the obtained passphrase. A file encryption key is generated and the digital data in the file encrypted with the file encryption key to provide an encrypted file. The file encryption key is encrypted with the personal key to provide an encrypted file encryption key.

Ko et al. is directed to a method of testing a digital mobile phone network comprising creating test traffic using an unmodified test mobile phone coupled to a computer, and using the computer to measure a parameter associated with the

network's response to the test traffic. The measurements made by the computer are encoded into the test traffic to create a data stream within the mobile phone network comprising test traffic, measurements relating to the test traffic, and signaling relating to the test traffic, whereby this data stream can be captured at points within the network and analysed to investigate the functioning of the network dynamically as the network is exercised with the test traffic.

Henderson et al. is directed to an improved telecommunication system capable of supporting an enhanced audio transmission mode and a conventional PCM waveform encoding mode. The telecommunication system performs an in-band signaling routine during a first communication session in accordance with the PCM protocol. The in-band signaling routine employs a form of robbed bit signaling to transmit information between the calling codec and the called codec. The signaling information is utilized to determine whether the called codec is compatible with the enhanced audio coding mode and to initiate the transition between the PCM mode and the audio coding mode.

Weinstein et al. is directed to the relative and absolute calibration for dosimetric devices. A first self-calibration curve relates a first array image to a first acquired image, the first array image being recorded from application of a first radiation treatment plan to a detector array, and the first acquired image being recorded from application of the first radiation treatment plan to a radiation detector. At least one subsequent self-calibration curve relates at least one subsequent array image, the subsequent array image, and the subsequent acquired image.

35 U.S.C. 112, Second Paragraph

Claim 14 has been amended to address the Examiner's rejection.

**The Claims Distinguish Patentably
Over the References of Record**

Claims 1-4 and 8-11 are patentable over Jutzi et al. in view of Parr in further view of Suzuki.

More specifically, regarding **claim 1**, Jutzi et al. does not disclose deriving a fingerprint from the decoded signal, comparing said fingerprint with fingerprints stored in a database, and concluding that the encoded signal has been encoded with said particular type of encoder if the derived fingerprint corresponds to

one of the fingerprints stored in the database. The Office Action refers Applicant to paragraphs [0047], [0048], and [0055]-[0056] which discloses a method for enabling secure content decryption with a set-top box. More specifically, a content decryption component receives a stream of encrypted content from a secured content driver. The content decryption component then performs integrity authentication of a run-time image of the secure content driver to determine if the secure content driver is authenticate. A run-time integrity authentication process calculates a hash value of the program instructions that perform the functionality of the secure content driver prior to loading the program instruction into memory. The process then determines whether the calculated hash values matches a pre-calculated hash value to determine whether the secure content driver is authenticate. When the hash value matches, the functionality of the secure content driver is performed otherwise the process is terminated. Jutzi et al. discloses authenticating secured content drivers by comparing hash values calculated from the program instructions. Jutzi et al. does not disclose deriving a fingerprint that used to derive if the encoded signal has been encoded with a particular type of encoder if the fingerprint corresponds to a fingerprint stored in a database. The Office Action asserts that the Parr teaches this limitation in Col. 1 lines 25-29 and Col. 2 lines 30-40 which discloses identification of an encoder type through the observation of the encoded data received. More specifically, encoded data is received by a receiver and the characteristic of the received encoded data identifies the type of encoder. The type of encoding is determined without decoding the received information. Parr does not disclose decoding the received signals and determining the type of encoder from a fingerprint that is derived from the decoded signal. Nor does Suzuki disclose deriving a fingerprint from a decoded signal and comparing the fingerprint to other fingerprints stored in a database. There is no evidence or suggestions in Jutzi et al., Parr, Suzuki, or the combination of deriving a fingerprint from a decoded signal and comparing the fingerprint to other fingerprints stored in a database to determine a type of encoder that encoded the signal, as advanced by the Examiner, except from using Applicant's claims as a template through a hindsight reconstruction of the Applicant's claims.

Accordingly it is submitted that independent **claim 1** and **claims 2-4** that depend therefrom distinguish patentable over the references of record.

Claim 4 calls for awarding the client if the server concluded that the received encoded signal has been encoded with said particular type of encoder

wherein the award is the database metadata associated with the signal. Neither Jutzi et al., Parr, Suzuki, nor the combination teach or disclose giving the client the database metadata associated with the signal if the server concluded that the signal has been encoded with the particular type of encoder.

Claim 8 calls for deriving a fingerprint from a decoded signal and then comparing the fingerprint with other fingerprints stored in the server's database to determine whether the signal was encoded with a particular type of encoder. It is respectfully submitted that Jutzi et al., Parr, Suzuki, or the combination does not teach or disclose deriving a fingerprint from a decoded signal and comparing the selected fingerprint with fingerprints in a server's database to determine a type of encoder used to encode the signal.

Claim 9 calls for a fingerprint extraction unit configured to extract the fingerprint from a decoded file and a processor configured to compare the extracted fingerprint with other fingerprints stored in a database. It is respectfully submitted that Jutzi et al., Parr, Suzuki, or the combination does not teach or disclose comparing fingerprints extracted from a decoded file with fingerprints stored in the server's database to determine the type of encoder used to encode the signal.

Accordingly it is submitted that independent **claim 9** and **claims 10-15** that depend therefrom distinguish patentable over the references of record.

Claim 11 calls for in response to the server concluding that the received encoded files have been encoded with an encoder that corresponds to the decoder of the server, the processor communicates an award to the client wherein the award includes metadata associated with the encoded file, the metadata being transmitted to the client. Neither Jutzi et al., Parr, Suzuki, nor the combination teach or disclose giving the client the database metadata associated with the signal if the server concluded that the signal has been encoded with the particular type of encoder.

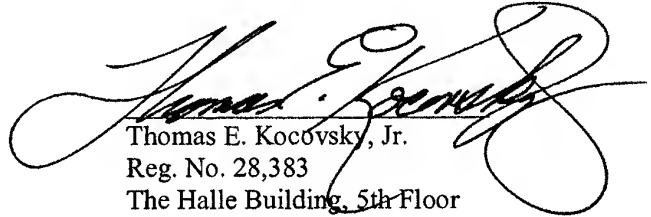
CONCLUSION

For the reasons set forth above, it is submitted that **claims 1-4 and 8-16** (all claims) distinguish patentably over the references of record and meet all statutory requirements. An early allowance of all claims is requested.

In the event the Examiner considers personal contact advantageous to the disposition of this case, the Examiner is requested to telephone Thomas Kocovsky at 216.363.9000.

Respectfully submitted,

Fay Sharpe LLP

A large, stylized handwritten signature in black ink, which appears to read "Thomas E. Kocovsky, Jr.", is written over the printed name and address.

Thomas E. Kocovsky, Jr.
Reg. No. 28,383
The Halle Building, 5th Floor
1228 Euclid Avenue
Cleveland, OH 44115-1843
216.363.9000